

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
IDENTITY THEFT

Before the

SUBCOMMITTEE ON TECHNOLOGY,
TERRORISM AND GOVERNMENT INFORMATION

of the

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

Washington, D.C.

March 7, 2000

Mr. Chairman Kyl, and members of the Subcommittee, I am Jodie Bernstein, Director of the Bureau of Consumer Protection, Federal Trade Commission (AFTC® or ACommission®).¹ I appreciate the opportunity to present the Commission's views on the important issue of identity theft, and describe to you the Commission's achievements in implementing the Identity Theft and Assumption Deterrence Act.²

In my remarks today, I will discuss the growing phenomenon of identity theft, how the Commission has responded to identity theft, both in carrying out its duties under the 1998 Act and its general enforcement measures, and what we see as future challenges in eradicating identity theft.

1. Identity Theft: A Growing Problem

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and response to questions are my own, and do not necessarily represent the views of the Commission or any Commissioner.

² Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. ' 1028).

By now, many people have confronted, directly or through a third person, some form of identity theft: someone has used their name to open up a credit card account or someone has used their identifying information -- name, social security number, mother's maiden name, or other personal information -- to commit fraud or engage in other unlawful activities. Other common forms of identity theft include taking over an existing credit card account and making unauthorized charges on it (typically, the identity thief forestalls discovery by the victims by contacting the credit card issuer and changing the billing address on the account); taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and using personal information to access, and transfer money out of, another person's bank or brokerage account. In extreme cases, the identity thief may completely take over his or her victim's identity -- opening a bank account, getting multiple credit cards, buying a car, getting a home mortgage and even working under the victim's name.³

Identity theft can arise from simple, low-tech practices such as stealing someone's mail or Dumpster diving through their trash to collect credit card offers or obtain identifying information such as account numbers or social security numbers. There are also far more sophisticated practices at hand. In a practice known as Skimming,⁴ identity thieves use computers to read and store the information encoded on the magnetic strip of an ATM or credit card when that card is inserted through either a specialized card reader or a legitimate payment mechanism (e.g., the card reader used to pay for gas at the pump in a gas station). Once stored, that information can be re-encoded onto any other card with a magnetic strip, instantly

³ In at least one case, an identity thief reportedly even died using the victim's name, and the victim had to get the death certificate corrected. Michael Higgins, *Identity Thieves*, ABA

transforming a blank card into a machine-readable ATM or credit card identical to that of the victim.

JOURNAL, October 1998, at 42, 47.

The Internet has dramatically altered the potential impact of identity theft. Among other things, the Internet provides access to collections of identifying information gathered through both illicit and legal means. The global publication of identifying details that heretofore were available only to the few increases the potential misuse of that information. Similarly, the Internet expands exponentially the ability for a third party to disseminate the identifying information, making it available for others to exploit. The recent reports of a Russian hacker gaining access to the names, addresses and credit card account numbers of hundreds of thousands of customers is an extreme example of the type of harm that can occur through the wholesale theft of identifying information. In this instance, the hacker posted the names and credit card numbers on a website, providing the wherewithal for others to commit identity theft by using those credit card numbers to make purchases.⁴

Anecdotes and news stories provide one indication of the growth of identity theft. Available statistics confirm this trend. The General Accounting Office, for example, reports that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35,235 in 1992 to 522,922 in 1997,⁵ and that the Social Security Administration's Office of the Inspector General conducted 1153 social security number misuse investigations in 1997 compared with 305 in 1996.⁶ In 1999, the telephone hotline established by the Social

⁴ John Markoff, *Thief Reveals Credit Card Data When Web Extortion Plot Fails*, N.Y. TIMES, January 10, 2000, at A1.

⁵ Calls to this department included precautionary phone calls, as well as calls from actual fraud or identity theft victims.

⁶ U.S. GENERAL ACCOUNTING OFFICE, IDENTITY FRAUD: INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED (May 1998). The Social Security Administration attributed the increase in investigations, in part, to the hiring of additional investigators.

Security Administration Inspector General received reports of almost 39,000 incidents of misuse of Social Security Numbers.⁷

⁷ While we have created a database to capture information from complaints to our new toll-free Identity Theft Hotline (discussed in greater detail below), our data are still too limited to allow us to draw any significant conclusions about the extent of identity theft.

For victims of identity theft, the costs can be significant and long-lasting. Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts,⁸ the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred, and he or she typically must spend numerous hours sometimes over the course of months or even years contesting bills and straightening out credit reporting errors. In the interim, the consumer victim may be denied loans, mortgages, a driver's license, and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is essential. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

2. The Federal Trade Commission's Authority

1. Overview

⁸ The Fair Credit Billing Act, 15 U.S.C. ' 1601 *et seq.* and the Electronic Fund Transfer Act, 15 U.S.C. ' 1693 *et seq.* limit consumers' liability for fraudulent transactions in connection with credit and debit cards, respectively.

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act (FTC Act), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.⁹ With certain exceptions, the FTC Act provides the Commission with broad civil law enforcement authority over entities engaged in or whose business affects commerce,¹⁰ and provides the authority to gather information about such entities.¹¹ The Commission also has responsibility under more than forty additional statutes governing specific industries and practices.¹²

⁹ 15 U.S.C. ' 45(a).

¹⁰ Certain entities such as banks, savings and loan associations, and common carriers as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. ' 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. ' 1012(b).

¹¹ 15 U.S.C. ' 46(a).

¹² In addition to the credit laws discussed in the text, the Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455,

which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

Two of the Commission's specific statutory mandates are particularly relevant in the context of identity theft. The Fair Credit Billing Act and Fair Credit Reporting Act each provide important protections for consumers who may be trying to clear their credit records after having their identities stolen. The Fair Credit Billing Act, which amended the Truth in Lending Act, provides for the correction of billing errors on credit accounts and limits consumer liability for unauthorized credit card use.¹³ The Fair Credit Reporting Act (FCRA[®]) regulates credit reporting agencies and places on them the responsibility for correcting inaccurate information in credit reports.¹⁴ In addition, entities that furnish information to credit reporting agencies have obligations under the FCRA to ensure the accuracy of the information they report.¹⁵ Finally, the FCRA limits the disclosure of consumer credit reports only to entities with specified permissible purposes[®] (such as evaluating individuals for credit, insurance, employment or similar purposes) and under specified conditions (such as certifications from the user of the report).¹⁶

B. The Commission's Involvement In Identity Theft Issues

As an outgrowth of its broader concern about financial privacy, the Commission has been involved in the issue of identity theft for some time. In 1996, the Commission convened two public meetings in an effort to learn more about identity theft, its growth, consequences, and possible responses. At an open forum convened by the Commission in August 1996, consumers

¹³ 15 U.S.C. ' ' 1601 *et seq.*

¹⁴ 15 U.S.C. ' ' 1681e, 1681i .

¹⁵ 15 U.S.C. ' 1681s-2.

¹⁶ 15 U.S.C. ' 1681-1681u.

who had been victims of this type of fraud, representatives of local police organizations and other federal law enforcement agencies, members of the credit industry, and consumer and privacy advocates discussed the impact of identity theft on industry and on consumer victims.

Subsequent press coverage helped to educate the public about the growth of consumer identity theft and the problems it creates. In November 1996, industry and consumer representatives met again in working groups to explore solutions and ways to bolster efforts to combat identity theft.

Having developed a substantial base of knowledge about identity theft, the Commission testified before this subcommittee in May 1998 in support of the Identity Theft and Assumption Deterrence Act. Following the passage of the Act, the Commission testified again, in April 1999, before the House Subcommittee on Telecommunications, Trade and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Commerce Committee. This latest testimony focused on identity theft in the financial services industry.

C. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act or the Act) addresses identity theft in two significant ways. First, the Act strengthens the criminal laws governing identity theft. Specifically, the Act amends 18 U.S.C. ' 1028 (Fraud and related activity in connection with identification documents) to make it a federal crime to:

knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.¹⁷

¹⁷ 18 U.S.C. ' 1028(a)(7). The statute further defines Ameans of identification@ to include Aany name or number that may be used, alone or in conjunction with any other

information, to identify a specific individual,⁹ including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

The second way in which the Act addresses the problem of identity theft is by focusing on consumers as victims.¹⁸ In particular, the Act requires the Federal Trade Commission to develop a centralized complaint and consumer education service for victims of identity theft. More specifically, the Act directs that the Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.¹⁹

III. Current Efforts: the FTC's Consumer Assistance Program

¹⁸ Prior to the passage of the Act, financial institutions rather than individuals tended to be viewed as the primary victims of identity theft because individual consumers' financial liability is often limited. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals, to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

¹⁹ Pub. L. No. 105-318 ' 5, 112 Stat. 3010 (1998) (codified at 18 U.S.C. ' 1028 note).

In enacting the Identity Theft Act, Congress recognized that coordinated efforts are essential because identity theft victims often need assistance from both government agencies at the national and state or local level, and private businesses. Accordingly, the FTC's role under the Act is primarily one of managing information sharing among public and private entities. The goals of the FTC's information clearinghouse²⁰ are fourfold: 1) to support criminal law enforcement efforts by collecting data in one central database and making referrals as appropriate²⁰; 2) to provide consumers with information to help them prevent or minimize their risk of identity theft; 3) to streamline the resolution of the credit and financial difficulties consumers may have when they become victims of identity theft; and 4) to enable analysis of the extent of, and factors contributing to, identity theft in order to enrich policy discussions. In order to fulfill the purposes of the Act, the Commission has begun implementing a plan that centers on three principal components:

(1) *Toll-free telephone line.* The Commission has established a toll-free telephone number, 1-877-ID THEFT (438-4338), that consumers can call to report incidents of identity theft. Consumers who call the Identity Theft Hotline receive telephone counseling from specially

²⁰ Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. The practices the Commission expects to focus its law enforcement resources on are those where the effect is widespread and where civil remedies are likely to be effective. See, e.g., *FTC v. J.K. Publications, Inc., et al.*, No. CV 99-00044 ABC (AJWx) (C.D. Cal., Mar. 16, 1999) (order granting preliminary injunction) (alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services); *FTC v. James J. Rapp and Regana L. Rapp, individually and doing business as Touch Tone Information Inc., et al.*, Docket No. CV 99-WM-783 (D. Colo., filed April 21, 1999) (alleging that defendants obtained private financial information under false pretenses).

trained FTC and contractor personnel to help them resolve problems that may have resulted from the misuse of their identities. In addition, the hotline phone counselors enter information from the consumers' complaints into a centralized database, the Identity Theft Data Clearinghouse. In operation since November 1, 1999, the Identity Theft Hotline has averaged over 400 calls per week.

Our aim with each consumer call is to provide the comprehensive information needed to guard against or resolve problems caused by identity theft, and to assist in streamlining the process for the consumer wherever possible. Although there is generally no way for consumers to avoid contacting the many creditors who may be involved, our goal is that consumers should be able to make a single phone call to our hotline to report the offense, receive the information and assistance they need, and have their complaints referred to the appropriate government agency.

In particular, consumers who are victims of identity theft receive specific information about how to try to prevent additional harm to their finances and credit histories. The phone counselors instruct the callers to contact each of the three credit reporting agencies to obtain copies of their credit reports and request that a fraud alert be placed on their credit report.²¹ We advise consumers to review the information on the credit reports carefully to detect any additional evidence of identity theft. The counselors also routinely inform callers of their rights under the Fair Credit Reporting Act and provide them with the procedures for correcting misinformation on a credit report. Consumers receive additional information telling them how to

²¹ These fraud alerts request that the consumer be contacted when new credit is applied for in that consumer's name.

contact each of the creditors or service providers where the identity thief has established or accessed an account, and to follow up in writing by certified mail, return receipt requested.

Where the identity theft involves Aopen end@ credit accounts,²² consumers are advised on how to take advantage of their rights under the Fair Credit Billing Act, which, among other things, limits their responsibility for unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector regarding debts left behind by the identity thief are advised of their rights under the Fair Debt Collection Practices Act, which limits debt collectors in their collection of debts.

In addition, the FTC phone counselors advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and prosecute identity thieves, and because getting a police report often helps consumers in demonstrating to would-be creditors and debt collectors that they are genuine victims of identity theft. Almost half the states have enacted their own identity theft laws, and our counselors, in appropriate circumstances, will refer consumers to other state and local authorities, to pursue potential criminal investigation or prosecution.

²² The Fair Credit Billing Act applies to Aopen end@ credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts such as loans or extensions of credit that are repaid on a fixed schedule.

(2) *Identity Theft complaint database.* As mentioned above, detailed information from the complaints received on the FTC's toll-free Identity Theft Hotline is entered into the FTC's Identity Theft Data Clearinghouse (AClearinghouse®). The Clearinghouse is designed to become a comprehensive, government-wide repository of information collected from victims of identity theft. In the near future, it will begin incorporating complaints received by other government agencies, such as the Social Security Administration. Consumers can also enter their own complaint information via the public user complaint form at www.consumer.gov/idtheft.²³

²³ See page 14, *infra* .

Having designed and built the Clearinghouse database itself, the Commission is now developing the tools to extract and analyze the information it contains.²⁴ The information collected in the Clearinghouse will provide the Commission with a better understanding of how identity theft occurs. In particular, we will look at whether certain types of transactions or business practices lead to greater opportunities for the theft of a person's personal information or facilitate the misuse of that information once obtained. As we begin to identify trends and patterns in the occurrence of identity theft, we will share this information with our law enforcement partners so that they may better target their resources.²⁵

Moreover, the Identity Theft Data Clearinghouse will be available to law enforcement agencies at the federal, state, and local level through a secure, web-based interface. The Commission expects that the Clearinghouse will allow the many agencies involved in combating identity theft to share data, enabling these offices to work more effectively to track down identity

²⁴ While Congress authorized the appropriation of such sums as may be necessary to carry out the FTC's obligations under the Identity Theft Act, Pub. L. No. 105-318 ' 5(b), 112 Stat. 310 (1998), no funds have been appropriated for the Commission's identity theft program. Our ability to fully build out our database, including making the information contained therein electronically available to our law enforcement partners, as well as our ability to perform sophisticated analyses of the data we collect, is contingent on the appropriation of adequate funds. Our budget requests for the next three years ask for funding of \$2.8 million to complete the development of the system and maintain our call handling and consumer education responsibilities. Appropriations at the requested level would enable us to handle 100,000 calls for FY2001, and 200,000 annually thereafter. We have, in addition, submitted a reprogramming request to provide \$625,000 in funds for FY2000. Of this request, which is now pending with the Appropriations Subcommittees, \$525,000 would be distributed to the agency's contract account, and \$100,000 to our equipment account.

²⁵ In addition to our collaborative work with our law enforcement partners, the Commission is looking for opportunities to work with private sector entities who are critical to addressing identity theft issues. For example, credit reporting agencies could provide substantial assistance by detailing for this project how their existing fraud operations and databases function, and how information could most efficiently be shared with them.

thieves and assist consumers.²⁶ Criminal law enforcement agencies could take advantage of this central repository of complaints to spot patterns that might not otherwise be apparent from isolated reports. For example, federal law enforcement agencies may be able to identify more readily when individuals may have been victims of an organized or large-scale identity theft ring.

²⁶ The Commission has successfully undertaken a similar effort with respect to consumer fraud. The FTC's Consumer Sentinel network is a bi-national database of telemarketing, direct mail, and Internet complaints accessible to law enforcement officials throughout the U.S. and Canada. Currently the Sentinel database contains more than 210,000 entries, and is used by more than 200 law enforcement offices, ranging from local sheriff's offices to FBI field offices.

In addition, the Clearinghouse will facilitate the referral process required by the Identity Theft Act. Building upon the Commission's experience in sharing data and making referrals to combat consumer fraud through its successful Consumer Sentinel network,²⁷ we envision making identity theft referrals in a variety of ways beyond simply referring individual callers to appropriate agencies. As mentioned above, Clearinghouse members will be able to access this secure database directly from their desktops in order to support their investigations. In addition, the Commission plans to disseminate complaint information through customized standard reports, extracting for our law enforcement partners the Clearinghouse complaints that meet the criteria they have designated. Finally, when, during the course of our own in-house data analysis, we identify trends or patterns in the data that appear to have ramifications for our law enforcement partners, we will notify them of that information. Numerous law enforcement agencies have already expressed an interest in receiving information and referrals in these ways.²⁸

²⁷ See *supra* note 26.

²⁸ Pursuant to the requirements of the Identity Theft Act, the FTC hopes to gain the cooperation of the three major credit reporting agencies to establish an analogous information sharing and referral system to allow us to refer complaints received on our toll-free number to individual credit bureaus for assistance or resolution, as appropriate.

(3) *Consumer Education.* The FTC has taken the lead in coordinating the efforts of government agencies and organizations to develop and disseminate comprehensive consumer education material for victims of identity theft, and those concerned with preventing identity theft.²⁹ The results of the FTC's efforts include both print publications and a website, located at www.consumer.gov/idtheft. This collaborative consumer education effort is ongoing; we hope to lead a similar joint effort with many of the private sector financial institutions that have an interest in preventing and curing the effects of identity theft.

The FTC's most recent publication in this area is a booklet entitled: *Identity Theft: When Bad Things Happen to Your Good Name*.³⁰ The 21-page booklet covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. In addition to our own initial distribution of this booklet, the Social Security Administration has ordered and plans to distribute 100,000 copies of the booklet. The Federal Deposit Insurance Corporation has also indicated that it will print and distribute the

²⁹ Among the organizations the FTC has brought into this effort are the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of Thrift Supervision, the Department of Justice, the U.S. Secret Service, the Federal Bureau of Investigation, the Postal Inspection Service, the Internal Revenue Service, the Social Security Administration, the Federal Communications Commission, the Securities and Exchange Commission, the U.S. Trustees, and the National Association of Attorneys General.

³⁰ In April, 1999 the FTC took the interim step of issuing a consumer alert, *Identity Crisis . . . What to Do If Your Identity Is Stolen*, which gives consumers an overview of what to do if they are victims of identity theft.

booklet.

The Identity Theft web page features a web-based complaint form, allowing consumers to send complaints directly into the Identity Theft Data Clearinghouse. The website also includes the comprehensive identity theft booklet as well as other publications, tips for consumers, testimony and reports, information on recent identity theft cases, links to identity theft-related state and federal laws, descriptions of common identity theft scams, and links to other organizations and resources.³¹

³¹ The *www.consumer.gov* site is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from 61 federal agencies. The consumer.gov project was awarded the Hammer Award in March 1999.

Finally, the Commission recognizes that the success of this effort hinges on the public's awareness of these resources. On February 17, 2000, the Commission announced its Identity Theft Program, promoting the toll-free number, the website and our consumer education campaign.³² We anticipate that we will see an increase in our call volume and website visits following these efforts to raise the public awareness of identity theft.

IV. Ongoing Issues

In May 1998, the Commission testified before this subcommittee in support of the Identity Theft and Assumption Deterrence Act. The Commission continues to believe that the Act is an important tool in addressing the problem of identity theft. Since its passage, the FTC has increased its efforts to develop a program to quantify the data regarding identity theft, to provide assistance to identity theft victims who seek help in resolving identity theft disputes, and provide consumers and others a central place in the federal government to go for information about identity theft. Already, in the relatively brief time our identity theft hotline has been operational, the FTC has assisted over 4000 consumers who have been, or are worried about becoming, victims of identity theft. We anticipate that our consumer assistance program will continue to expand and grow over the coming months.

³² While the toll-free number has been operational since November 1999, we waited several months to make a major announcement in order to fully train the telephone counselors, and otherwise smooth out the data collection operations. Even without a formal announcement, the toll-free line has received an average of 400 calls per week.

Notwithstanding our efforts and those of other law enforcement agencies, however, identity theft continues to pose significant problems for consumers. Some preliminary areas of concern to the Commission are as follows:

Prevention. Although many bank, credit card issuers, and other companies have put into place extensive systems to guard against identity theft, there nonetheless remain a number of continuing practices that may contribute to the problem of identity theft. Fraud alerts, for instance, are not foolproof. Identity thieves may be able to open accounts in the victim's name notwithstanding a fraud alert either because the fraud alert is not picked up by the credit scoring or other automated system used by the new creditor, or because the creditor fails to take sufficient precautions to verify the applicant's legitimacy when presented with a fraud alert. One caller to the FTC's hotline whose wallet had been stolen, for example, reported that after placing a fraud alert on her credit reports, at least seven fraudulent accounts were opened in her name at various retail establishments that granted instant credit³³ based only on a credit score that did not take into account fraud alerts.³³

³³ Of course, it is important to the prevention of identity theft that creditors pay attention and follow-up with appropriate verification procedures wherever there are possible indicia of fraud. One Arlington, Virginia resident who called the FTC had been disturbed to find that her ATM card no longer worked. When she called her bank, she learned that someone using her name had reported her card lost, and asked that a replacement card be sent -- to Brooklyn, New York. The sudden change-of-address presumably should have raised a red flag, but, in fact,

apparently triggered no further investigation. Such oversights, often committed out of an understandable desire to provide prompt customer service, do not appear to be uncommon.

In addition, although individual credit issuers have systems to detect automatically unusual patterns of activity, it is more difficult to detect unusual activity across creditors. Thus, for example, if an identity thief opens 30 different credit accounts in the course of 2 days, none of the 30 individual creditors may notice anything unusual. However, taken as a whole, the pattern of activity would likely trigger suspicion. Thus, one possible area for further action lies in bringing together creditors and credit reporting agencies (the group that is probably best placed to notice when there have been numerous credit applications or new accounts opened) to develop mechanisms for detecting such fraud -- and thus heading off identity theft.

Remediation. Identity theft victims continue to face numerous obstacles to resolving the credit problems that frequently result from identity theft.³⁴ For example, many consumers must contact and re-contact creditors, credit bureaus, and debt collectors, often with frustrating results. Using the data collected from consumer complaints, the Commission is actively monitoring the nature and extent of problems reported by consumers, and looking at possible means of addressing these problems, including ways of streamlining the remediation process.

In particular, the FTC believes that, as a first step, it would benefit consumers if they could make a single phone call -- presumably, to any of the major credit bureaus or to the FTC's hotline -- and have a fraud alert placed on all three of their credit reports, and copies of each of

³⁴ Some identity theft victims face significant, non-credit-related problems as well. For example, in a small but troubling number of cases, consumers calling the FTC's toll-free number have reported that they themselves have been arrested because of something an identity thief did while using their name, or that they learned they had a criminal arrest or conviction on record because an identity thief used identification with their name rather than his or her own when arrested for committing some other crime. Needless to say, correcting legal arrest or conviction

their three reports sent to their home address. The success of such an effort depends on the cooperation of the major credit bureaus.³⁵

As the FTC's new identity theft program expands, the Commission will have more data and experience from which to draw in determining what additional actions may need to be taken to best assist identity theft victims.

V. Cooperative Efforts

The Commission has been working closely with other agencies in a number of ways to establish a coordinated effort to identify the factors that lead to identity theft, work to minimize those opportunities, enhance law enforcement and help consumers resolve identity theft problems. In April 1999, for example, Commission staff held a meeting with representatives of 17 federal agencies as well as the National Association of Attorneys General to discuss implementing the consumer assistance provisions of the Identity Theft Act. In addition, FTC staff participates in the identity theft subcommittee of the Attorney General's Council on White

records can prove extremely difficult.

³⁵ Another question potentially raised by the experiences of identity theft victims is whether the protections currently afforded by laws such as the Fair Credit Reporting Act and Fair Credit Billing Act are adequate for resolving the problems commonly faced by identity theft victims. Because the data the Commission has gathered in the short time its hotline has been operational are limited, it would be premature to try to resolve such questions at this time.

Collar Crime, which has, among other things, developed guidance for law enforcement field offices on how best to assist identity theft victims. FTC staff also coordinates with staff from the Social Security Administration's Inspector General's Office on the handling of social security number misuse complaints, a leading source of identity theft problems.

Furthermore, almost half of the states have now enacted their own statutes specifically criminalizing identity theft. Others have passed, or are considering, further legislation to assist victims of identity theft,³⁶ including legislation specifically designed to help victims clear up their credit records.³⁷ The Commission is committed to working with states and local governments on this issue, and learning from their efforts.

Most recently, FTC staff has been assisting the Department of Treasury on plans for the upcoming National Summit on Identity Theft on March 15-16. The Summit provides a significant opportunity for government and business leaders to develop partnerships to combat identity theft and assist its victims.

VI. Conclusion

The Commission, working closely with other federal agencies and the private sector, has

³⁶ See, e.g., Iowa Code ' 714.16B (creating a private right of action for victims of identity theft).

³⁷ See Cal. Civ. Code ' 1785.6 (providing that if a consumer provides a credit bureau with a copy of police report of identity theft, the credit bureau shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of Section 530.5 of the Penal Code [the California identity theft statute] so that the information cannot be reported; the information may be unblocked only upon a preponderance of the evidence establishing that the information was blocked due to fraud, error, or that the consumer knew or should have known that he or she obtained goods, services, or moneys as a result of the blocked transactions).

already made strides towards identifying ways to reduce the incidence of identity theft. More focused law enforcement, greater consumer education and increased awareness by the private sector will all contribute to this effort. The FTC also looks forward to working with the Subcommittee to find ways to prevent this crime and to assist its victims.